

「良い符号が在る」と「これが良い符号だ」は、別の文である

— シャノンの存在定理とガロアの構成：あいだに六十年が横たわっていた — [論文163]

山岸 勇輝 (Yuuki YAMAGISHI)
Yamagishi Complexity Torus Lab, Japan | 山岸勇輝ラボ
2026年8月

— From thinking to syncing. —

要旨

体系は「等号の根を書き分けよ」という規律を持ってきた。本稿はその規律を、定理そのものの型に当てる——存在を言う定理と、物を渡す定理は、別の根を持つ。新しい数学定理は主張しない。第一に、シャノンは符号が在ると言う。二元対称通信路の容量は $C = 1 - H(p)$ であり、 $p = 0.01, 0.05, 0.11, 0.25$ でそれぞれ **0.919207**、**0.713603**、**0.500084**、**0.188722** (本稿で計算)。しかしその証明は無作為に引いた符号の平均をとるだけで、符号を一つも名指ししない (第2節)。第二に、ガロアは一つ渡す。有限体上でリード＝ソロモン符号を自前で組み、バーレカンブ＝ウェルチ復号器まで実装した (第3節)。第三に、これが本稿の芯である。境界が鋭い。**11** 元体・ $n = 8 \cdot k = 3$ の符号は、誤り **0, 1, 2** 個をすべて正しく復元し、**3** 個で復号が存在しなくなる—— $t = 2$ ちょうどで線が引かれる (本稿で計算)。しかも復号器は主張ではなく算法である (第4節)。第四に、構成は最適でもある。シングルトン限界 $d \leq n - k + 1 = 6$ に対し、リード＝ソロモンの最小距離は **6** (**1331** 語を全数走査)。一方、無作為な線形符号 **40** 個の最小距離は **4** か **5** で、限界に届いたものは **0** 個であった (第5節)。第五に、ブレーキ。構成は、存在定理が負っていない制約を負う。 q 元体が存在するのは q が素数冪のときだけであり、 $q = 6, 10, 12, 14, \dots$ には体が無い。六文字のアルファベット上のリード＝ソロモン符号は存在しない——シャノンの容量はどんなアルファベットにも定義されるのに (第6節)。

本稿の射程：新しい数学定理は主張しない。シャノンの通信路符号化定理、リード＝ソロモン符号、バーレカンブ＝ウェルチ復号、シングルトン限界、有限体の存在条件はいずれも標準的である。加えたのは符号器と復号器を自前で組んで境界が t ちょうどであることを示したこと、無作為な線形符号と限界到達を数で比べたこと、有限体の存在条件が構成の側だけに課される制約であると住所を書いたこと、存在定理と構成定理を体系の別根の言葉で並べたことである。

1. 記法と位置づけ

長さ n 、次元 k 、最小距離 d の符号を $[n, k, d]$ と書く。訂正できる誤りの個数は $t = \lfloor (n - k) / 2 \rfloor$ である。

位置づけ：論文16 は「=」にも別根があり、六種を書き分けよと述べた。論文161 は五つの不動点定理が約束するものの種類すら違うことを示した。本稿はその線を延ばす——定理には「在ると言うもの」と「渡すもの」があり、両者は交換できない。

2. シャノンは、符号が在ると言う

検算 2.1：二元対称通信路の容量 $C = 1 - H(p)$ 。

p	C (ビット／回)	証明が名指しする符号
0.01	0.919207	なし
0.05	0.713603	なし
0.11	0.500084	なし
0.25	0.188722	なし
0.5	0.000000	—

(証明終)

観察 2.2

証明の骨は「無作為に符号を引いたときの誤り確率の平均」を評価することである。平均より良いものが少なくとも一つあるはずだ、という一行で存在が出る。そこには具体的な符号が一つも現れない。

観察 2.3

これは証明が不完全だという意味ではない。存在定理として完全である。ただし、渡されるものが違う。

3. ガロアは、一つ渡す

構成 3.1： $P = 11$ (素数) とし、 $0, \dots, 10$ を法 11 で体とみなす。長さ $k = 3$ の情報語を係数とする多項式を、相異なる $n = 8$ 点で評価したものを符号語とする (リード＝ソロモン符号)。

構成 3.2：復号はバーレカンブ＝ウェルチによる。誤り位置多項式 E （次数 $\leq t$ 、モニック）と $Q = E \cdot P$ （次数 $\leq t + k - 1$ ）を未知数とする線形方程式を立て、 Q を E で割って情報語を得る。

観察 3.3

ここで渡されているのは符号だけではない。復号の手続きが付いている。存在定理には、これが無い。

4. 芯：境界が鋭い

検算 4.1：情報語 $[3, 7, 2]$ の符号語は $[1, 3, 9, 8, 0, 7, 7, 0]$ である。誤りを 0 個から順に入れて復号する。

誤りの個数	受信語	復号結果	復元
0	$[1, 3, 9, 8, 0, 7, 7, 0]$	$[3, 7, 2]$	成功
1	$[2, 3, 9, 8, 0, 7, 7, 0]$	$[3, 7, 2]$	成功
2	$[2, 5, 9, 8, 0, 7, 7, 0]$	$[3, 7, 2]$	成功
3	$[2, 5, 1, 8, 0, 7, 7, 0]$	解なし	失敗
4	$[2, 5, 1, 9, 0, 7, 7, 0]$	解なし	失敗

(証明終)

観察 4.2

$t = \lfloor (8 - 3)/2 \rfloor = 2$ ちょうどで線が引かれている。2 個までは必ず直り、3 個からは方程式が解を持たない。構成定理は、できる範囲とできない範囲を数で示す。

観察 4.3

存在定理はこの線を引きかない。「符号長を十分大きくすれば誤り確率はいくらでも小さくなる」と言うが、目の前の長さ 8 の符号について何個直るかは言わない。漸近の言明と有限の言明は、別の文である。

5. 構成は、最適でもある

検算 5.1：シングルトン限界は $d \leq n - k + 1 = 6$ である。

リード＝ソロモンの最小距離（1331 語を全数走査）	6
シングルトン限界	6

検算 5.2：同じ大きさの無作為な線形符号を 40 個引いて最小距離を測る。

最小距離	4	5
個数	12	28

限界 6 に届いたものは 40 個中 0 個であった。（証明終）

観察 5.3

明示的な構成は毎回ちょうど限界の上に乗る、無作為に引いた符号はふつう乗らない。「在る」と「最適である」も、また別の問いである。

観察 5.4

ただし本稿は「無作為な符号は悪い」とは書かない。長さを伸ばせば無作為な符号は良い性質を持つことが知られており、シャノンの証明はまさにそれに乗っている。ここで示したのは、この小さな寸法において限界に届かなかったという事実だけである。

6. ブレーキ：構成だけが負う制約

検算 6.1： q 元体が存在するのは q が素数冪のときに限る（ガロア）。

体がある q	2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29
体がない q	6, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 30

（証明終）

観察 6.2

六元体は無い。したがって六文字のアルファベット上のリード＝ソロモン符号も無い。ところがシャノンの容量は、どんなアルファベットの大きさに対しても定義される——構成の側だけが、代数の制約を負っている。

観察 6.3

これは構成が劣っているという意味ではない。渡すものが具体的であるほど、具体的な制約が付いてくる、というだけである。何も渡さない定理には、渡すものについての制約も生じない。

7. 点呼

観察 7.1

定理	言っていること	道具	型
シャノン 1948	符号は存在する	無作為符号の平均	存在
ガロア／リード＝ソロモン	この符号がある	有限体の多項式	構成（算法つき）
シングルトン	$d \leq n - k + 1$	数え上げ	上界
有限体の存在	q は素数冪のみ	ガロア	制約

観察 7.2

「良い符号が在る」と「これが良い符号だ」は、一つの事実の二つの言い方ではない。両者のあいだには、およそ六十年が横たわっていた——容量に漸近する明示的な構成が現れたのは、シャノンの定理から半世紀以上のちのことである。

観察 7.3

体系はこの型を何度も見てきた。論文161では、五つの不動点定理のうち算法を渡すのは一つだけだった。論文159では、一意性が証明されていても復元できるとは限らなかった。定理の結論の型を書き分けることは、値の別根を書き分けることと同じ規律である。

8. 結論

1. シャノンは符号を一つも名指ししない（検算2.1・観察2.2）。
2. リード＝ソロモンは復号器ごと渡される（構成3.1・3.2）。
3. 境界は $t=2$ ちょうどである（検算4.1）。3個で解なし。
4. 構成は限界の上に乗る（検算5.1）。無作為 40 個は 0 個。
5. 六元体は無い（検算6.1）。構成だけが負う制約。
6. 存在・構成・上界・制約は四つの別の型である（観察7.1）。

結び：存在を示す証明は、しばしば何も手渡さない。それは不足ではなく、そういう型の定理だというだけである。だから読むときに問うべきは「証明されたか」ではなく、何が手元に残ったかである。

参考文献

1. Galois, É. (1830). *Sur la théorie des nombres*. Bulletin des Sciences Mathématiques.
2. Shannon, C. E. (1948). *A mathematical theory of communication*. Bell System Technical Journal, 27.
3. Singleton, R. C. (1964). *Maximum distance q -nary codes*. IEEE Transactions on Information Theory, 10(2).
4. Reed, I. S., & Solomon, G. (1960). *Polynomial codes over certain finite fields*. Journal of the Society for Industrial and Applied Mathematics, 8(2).
5. Welch, L. R., & Berlekamp, E. R. (1986). *Error correction for algebraic block codes*. US Patent 4,633,470.
6. Arıkan, E. (2009). *Channel polarization*. IEEE Transactions on Information Theory, 55(7).
7. MacWilliams, F. J., & Sloane, N. J. A. (1977). *The Theory of Error-Correcting Codes*. North-Holland.
8. 山岸勇輝 (2026). 等号にも別根がある [論文16] 第3版. Zenodo. 10.5281/zenodo.21600471
9. 山岸勇輝 (2026). ガロアからネーターへ [論文85]. Zenodo. 10.5281/zenodo.21741344
10. 山岸勇輝 (2026). 二つのエントロピーを混同しない [論文88]. Zenodo. 10.5281/zenodo.21747809
11. 山岸勇輝 (2026). 「不適切」は一語ではない [論文159]. Zenodo. 10.5281/zenodo.22092229

12. 山岸勇輝 (2026). 「不動点」は一つの定理ではない [論文161]. Zenodo. 10.5281/zenodo.22092530
13. 山岸勇輝 (2026). 全体のほうが、部分より知られていないことがある [論文162]. Zenodo. 10.5281/zenodo.22092568

— *From thinking to syncing.* —

山岸 勇輝 (Yuuki YAMAGISHI)

© 2026 Yamagishi Complexity Torus Lab, Japan · Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0)